IN THE CLAIMS

1. (Original) A method for generating web traffic reports comprising the steps of:

presetting IP filters;

storing a web page on a first server coupled to a wide area network, said web page including data mining code;

uploading the web page to a visitor computer responsive to a request over the wide area network from the visitor computer, said visitor computer having a designated IP address;

operating the data mining code on the visitor computer to obtain technical data;

receiving at a second server the technical data and the IP address of the visitor computer and generating a log file incorporating the technical data and IP address;

applying the IP filters to the IP address stored in the log file; and

generating a database file from the log file responsive to the IP filters.

2. (Original) The method of claim 1, wherein the step of presetting IP filters includes setting an INCLUDE IP filter.

3. (Original) The method of claim 1, wherein the step of presetting IP filters includes setting an EXCLUDE filter.

4. (Original) The method of claim 1, wherein the step of applying the IP filters to the IP addresses includes the step of using classless inter-domain routing.

5. (Original) The method of claim 1, wherein the step of applying the IP filters to the IP addresses includes the step of using standard pattern matching specifications like Regular Expressions.

6. (Original) The method of claim 1 further including the steps of:

defining a subnet mask; and

filtering the IP addresses using the subnet mask with a binary AND operator.

7. (Original) A network comprising:

a visitor node having a browser program coupled to said network, said visitor node providing requests for information on said network;

a web site node having a respective web site responsive to requests for information from said visitor node to provide media content and data mining code to said visitor node;

a tracking node including a log file and a database, said tracking node responsive to a communication from said visitor node based upon said data mining code to store visitor data obtained from said visitor node into said log file; and

a filter node responsive to said visitor data based on a filter to select said visitor data for storage in a database,

whereby said database is accessible by an owner of said web site node to view relevant traffic data to the web site node.

8. (Original) A network in accordance with claim 7, wherein said filter node selects said visitor data based on whether the visitor data is included within the filter.

9. (Original) A network in accordance with claim 7, wherein said filter node selects said visitor data based on whether the visitor data is excluded from the filter.

10. (Original) A network in accordance with claim 7, wherein said filter is an IP address filter.

11. (Original) A network in accordance with claim 7, wherein said filter is a subnet mask applied to an IP address of the visitor node using an AND operator.

12. (Original) A network in accordance with claim 7, wherein said filter uses classless inter-domain routing.

13. (Original) A network in accordance with claim 7, wherein said filter uses standard pattern matching specifications like Regular Expressions.